NASA Risk Management for IT Security

NASA Risk Management Conference V

October 26-29, 2004

Tom Siu, RS Information Systems

GRC Network Security Team

tjsiu@grc.nasa.gov

Objectives

- The Progression of NASA IT Security Risk Assessment and Risk Management Program
  - Where we have been
  - Changes in Federal laws
  - Where we are headed
  - Why CRM
  - Characteristics of IT Security risks
  - What you should expect from IT Security Risk Assessment

2002 OIG and GAO IT Security Findings

The lack of a consistent approach to conducting, analyzing, and documenting risk assessments. The agency needs to standardize on a product or an approach to help prevent threats from being totally overlooked due to inexperience in performing assessments and analysis.

Where We Have Been

- NPG 2810.1 - “Security of Information Technology”
- IT Security Plans- all NASA systems, due Sep 30, 2001
- NPG 8000.4 and NPG 7120.5 refer to NPG 2810.1 for IT security risk management

- IT Security risk assessments inconsistent across NASA
  - Using NPG 2810 Appendix A as taxonomy questionnaire
  - Comparing ‘set analysis’ of ‘best security practices’
  - Not updated with the pace of change in the IT world
  - Not looking for risks, but controls not in place, regardless of environment

Why Inconsistent Risk Management ?

- Follow the money
  - Programs and Projects fund IT systems
  - NASA CIO responsible for IT infrastructure
- 11 different visions of risk tolerance (Center specific)
- IT and IT security staff not familiar with formal risk management (CRM) at NASA
- Some “management to reports” rather than risk management
- Not a Project Management culture or focus
- Ideally: IT Security and Information Security
  - Balance security with connectivity and functionality

Changes in Federal Laws

- Federal Information Security Management Act of 2002 (FISMA)
  - Requires IT security practice to be based on
    - Risk assessments
    - Risk managed approach to manage IT infrastructure & systems
  - Dictates compatibility with NIST guidelines for ALL Federal Agencies
    - NIST Special Publication 800-30 - Risk Management
    - Use of CRM is consistent with NIST SP 800-30
- Can no longer use cursory risk assessments in IT security planning.
- Certification and Accreditation requirements increase costs and effort levels for IT security planning
- CAIB Report- subsystems risk correlation

Where We Are Headed

- The new NPR 2810.1A (DRAFT) driving toward “continuous” approach to risk management.
- Agency Wide Applications- move IT risk decisions beyond Center local risk tolerance- have Agency wide impacts
  - IRIS
  - ODIN Consolidated Help Desk
  - OneNASA Portals
- Shifting to use CRM for IT security (at GRC)
  - Not unanimous with IT security practitioners
  - Deputy CIO for IT Security interested in promoting this approach
  - Need an Agency IT Security Risk Manager
    - CIO, Safety & Mission Assurance, Chief Engineer, Security and Program Protection: it’s a big job

Why CRM ?

- Project risks will overshadow IT security risks
- Using the CRM approach and language permits IT security risks to be managed by the project manager
- Consistency for NASA the long term goal
  - For RM professionals
  - For IT Security professionals
    - Federal compatibility with NIST
- Adaptable to rapid change in IT arena
  - Threats change on a daily basis

IT Security Risk

Condition: a combination of
-Threat source
-Vulnerability

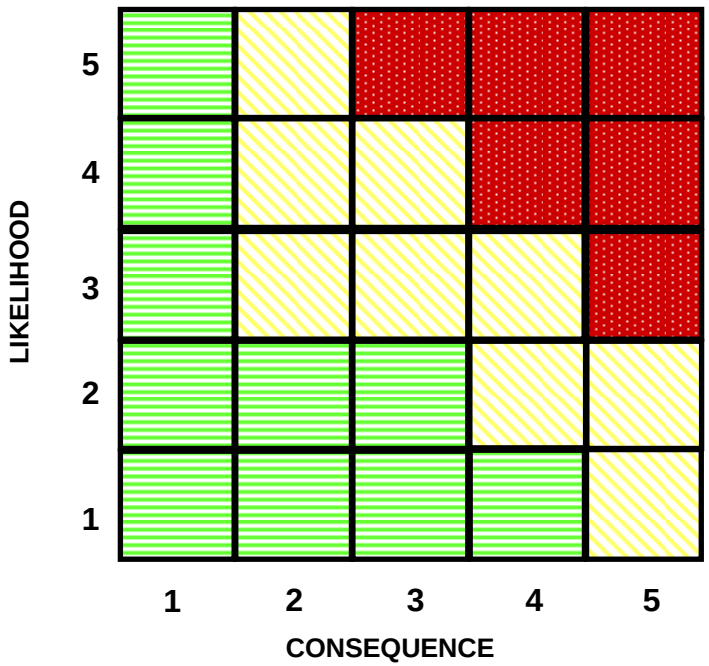
Consequence: Impact
-Disclosure
-Modification
-Loss/Destruction
-Interruption of service

Qualitative or Quantitative

Qualitative or Quantitative

Risk = Likelihood * Severity

IT Security Risk Matrix



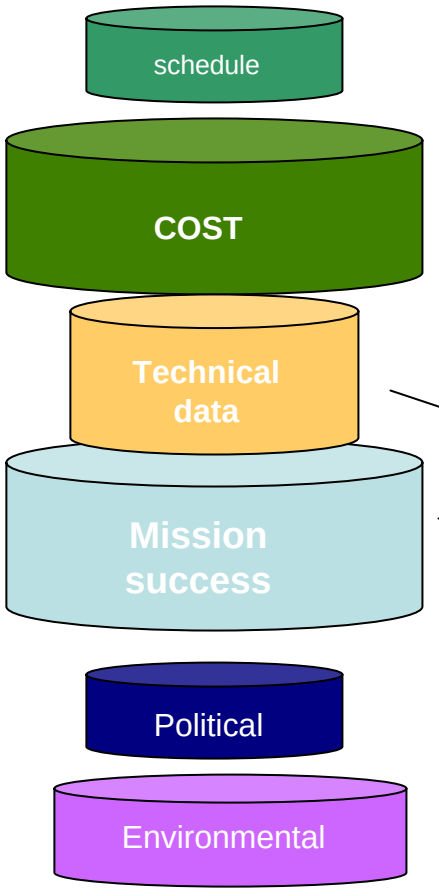
Properties of IT Security Risks

- Infrastructure risks impact multiple projects and programs
  - Data driven attacks, SQL slammer worm example
- Condition-to-consequence timeframes can be on the order of 5 days or less
- Can have a high cost to mitigate.
- Can cross Centers and NASA partners
  - Examples
- Hard to quantify- analysis is highly qualitative
- People sourced, technology impacted
- Projects could use multiple systems, multiple infrastructures
- Follow the information trail vs. technology trail

What You Should Expect From NASA IT Security Professionals

- Facilitate CRM-based risk assessments
  - No longer ask vendors/systems administrators/project teams to do their own risk assessments.
- Assist you with identification of Top Risks
  - Include infrastructure risks to your projects
- Provide guidance with the IT security planning processes
- Have a good understanding of the local threat environments of networked information systems
- Provide liaison with Security and Program Protection information security staff
- Be responsible (through NASA and Center CIOs) for IT infrastructure risks

Program Manager's Perspective



Project Risk Stack

- Decision making authority
- Information owner

IT Security

- Use CRM language
- IDENTIFY and insert IT Security related risks in to Program's Risk Management
- Working security issues from the inside vs. outside
- Rigorous focus of IT Security Expertise

Summary

- NASA has a very mature risk management program in CRM
- CRM is consistent with Federal IT security risk management directives
  - Common taxonomy between Project Managers and IT/IT Security
- Need NASA Safety and Mission Assurance, at the Agency level, to champion CRM to CIO for IT security
- Agency-wide IT applications are the drivers
- Improved management of IT security risks across the Agency

Questions

References

- SOLAR Risk Assessment Introduction- under Safety and Mission Assurance, Risk Management Overview CBT
- NPG 8705 Risk Management Procedures and Guidelines
- NPG 7120.5A NASA Program and Project Management Processes and Requirements
- Process Based Mission Assurance site- risk mgt plans: http://pbma.hq.nasa.gov/sma/SMA_PM_RMP.html
- NPR 2810.1A Draft- currently not yet in NODIS for review